



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/539,421	03/30/2000	Yasuhiro Mitsui	32165-159044	8177
26694	7590	01/20/2004	EXAMINER	
VENABLE, BAETJER, HOWARD AND CIVILETTI, LLP			TRAN, ELLEN C	
P.O. BOX 34385			ART UNIT	PAPER NUMBER
WASHINGTON, DC 20043-9998			2134	S
DATE MAILED: 01/20/2004				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/539,421	MITSUI, YASUHIRO
	Examiner Ellen C Tran	Art Unit 2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 30 March 2000.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-63 is/are pending in the application.
 - 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) _____ is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.
- 13) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.
 - a) The translation of the foreign language provisional application has been received.
- 14) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

**NORMAN M. WRIGHT
PRIMARY EXAMINER**

Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s). _____
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449) Paper No(s) <u>3</u>	6) <input type="checkbox"/> Other: _____

DETAILED ACTION

1. This action is responsive to communication: original application filed 30 March 2000 with a foreign priority date of 30 March 1999.
2. Claims 1-63 are currently pending in this application. Claims 1-5, 11-13, 16-18, 21-29, 34, 35, 43, 44, 49, 50, 52, 533, 58, 59, 61, and 62 are independent claims.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

4. Claims 1-20 are rejected under 35 U.S.C. 102(a) as being anticipated by Mintzer et al. U.S. Patent No. 5,875,249 (hereinafter '249).

5. **As to independent claim 1, “An image processing system comprising: an image providing apparatus (i.e. stamping process) which provides an image file, from which a digital watermark information can be extracted by using a watermark key that includes an authentication information which authenticates said image file provided by an valid provider (i.e. ownership of an image)” is taught in '249 col. 3, lines 27-38 “The present invention relates to a system and a method to verify an image through an “invisible watermark” that is stamped onto an image for image content verification ... The system consists of a stamping process that**

embeds digital information, called stamping information, into a source image based upon a defined mapping process to produce a stamped image. The mapping process is identified by a decoding "key" which allows a user to decode the stamping information from the stamped image, and this key is called a verification key. The system also includes a verification process that extracts stamping information from a stamped source image based upon the mapping process identified by the verification key ... Finally, the stamping information can be displayed to show the proper ownership of an image which is stamped";

"said watermark key of said image file; and an image utilizing apparatus which extracts said digital watermark information from said image file provided by said image providing apparatus using said watermark key provided by said image providing apparatus" is disclosed in '249 col. 3, lines 44-50 "into a source image based upon a defined mapping process to produce a stamped image. The mapping process is identified by a decoding "key" which allows a user to decode the stamping information from the stamped image, and this key is called a verification key. The system also includes a verification process that extracts stamping information from a stamped source image based upon the mapping process identified by the verification key";

"verifies whether said watermark key has been tampered or not using said authentication information in said watermark key, verifies whether said image file has been tampered or not using said verified watermark key and displays said verified image file" is shown in '249 col. 4, lines 53-61 "This extraction begins by

computing the watermark extraction function, $WX(*)$, from the verification key, and applies the function to every pixel $SS(I,J)$ to produce the watermark pixel $EW(I,J)$. The watermark extraction process is repeated until every pixel in the stamped-source image has been processed. The result is an extracted watermark image. This image can be compared visually or numerically with the original watermark image to check for alterations and discrepancies in the stamped image".

"and displays said verified image file" is shown in '249 col. 6, lines 45-48 "The stamping information can be extracted with the proper verification keys and displayed in the clients' computer systems".

6. **As to independent claim 2, "which generates a watermark key which"** is taught in '249 col. 4, lines 47-49 "A verification key is produced, together with the stamped image as the final products"

"includes an authentication information that authenticates said image file provided by said valid provider" is shown in '249 col. 3, lines 37-38 "In addition, the watermark inserted, though invisible, can be later extracted to show the ownership information";

the remainder of claim 2 contains the exact text as in claim 1 and is rejected as stated above.

7. **As to independent claim 3, "embeds a digital watermark, which can be extracted by using said watermark key, in said image file, and provides said image file and said watermark key; "** is taught in '249 col. 4, lines 33-50 "In the invisible image stamping process, the watermark image, $W(I,J)$ is embedded into the

source image, $S (I,J)$, to produce a stamped source image $SS (I,J)$ (I and J integers locating a particular value in a matrix and representing, for example, I th column and J th row). Each pixel in the source image is processed in turn. The processing applies a watermark extraction function $WX (*)$ to the selected pixel, and tests the extracted watermark value to determine whether it is equal to the value of the watermark to be embedded. If they are equal, the processing proceeds to the next pixel. If they are not equal, the value of the selected pixel is altered until the value of the extracted watermark is equal to the value of the watermark to be embedded, the change required to do this is calculated, and the negative of that change is propagated to pixels not yet processed using error diffusion. This process is repeated until every pixel in the source image has been stamped. A verification key is produced, together with the stamped image as the final products”;

“an image managing apparatus stores said verified image file and” is shown in ‘249 col. 6, lines 36-37 “The stamped images can be stored in a image archive 106, and subsequently can be retrieved by the image server 108”;

“said verified watermark key, and provides verified watermark key to a user; said verified image file and said verified watermark key to a user” is disclosed in ‘249 col. 6 lines 39-45 “The server controls and distributes the stamped images upon request, via the computer networks 109 which can be local-area networks or wide-area networks such as the Internet, to individual computer systems 110 connected to the network. The server 106 also controls the access to the verifications keys and distributes the proper key to the rightful client of any particular image”;

“which extracts said digital watermark information from said image file provided by said image managing apparatus using said watermark key” is taught in ‘249 col. 6, lines 45-47 “The stamping information can be extracted with the proper verification keys and displayed in the clients' computer systems”;

the remainder of claim 3 contains the exact text as previously claimed in claim 1 and 2 and is rejected as stated above.

8. **As to independent claim 4**, the claim contains the exact text as previously claimed in claims 1 thru 3 and is rejected as stated above.

9. **As to independent claim 5**, “associates an additional information, which includes an authentication information that authenticates said image file provided by said valid provider, with said image file and provides said image file with said additional information to a user” is taught in ‘249 col. 3, lines 27-38 “The watermark consists of the stamping information, and the image stamping process combines the watermark with the source image values without generating any visible traces of the watermark or any visual artifacts in the image. In other words, the watermark is perceptually invisible. Because it is invisible, any modification on the image alters the watermark, but unlike visible features, the attacker cannot restore the altered invisible mark stamped onto the image. The content of an image can then be verified for authenticity. In addition, the watermark inserted, though invisible, can be later extracted to show the ownership information”;

“extracts said authentication information from said additional information” is shown in ‘249 col. 3, 47-50 “The mapping process is identified by a decoding "key"

which allows a user to decode the stamping information from the stamped image, and this key is called a verification key. The system also includes a verification process that extracts stamping information from a stamped source image based upon the mapping process identified by the verification key”;

the remainder of claim 5 contains the exact text as previously claimed in claims 1 thru 4 and is rejected as stated above.

10. As to dependent claim 6, “generates said authentication information which authenticates said image file provided by said valid provider, and compares said generated authentication information with an authentication information extracted from said provided watermark key to verify whether said provided watermark key is valid” is shown in '249 col. 3, lines 54-60 “This watermark image permits visual comparison of the stamping information extracted in the verification process with the stamping information applied in the stamping process. In another embodiment, this comparison may also be performed by computer algorithm. Finally, the stamping information can be displayed to show the proper ownership of an image which is stamped.”

11. As to dependent claims 7-9, the claims contain the exact text as previously claimed and are rejected as stated above.

12. As to dependent claim 10, “wherein said authentication information includes a provider identifying information which identifies said provider of said image file or an image identifying information which identifies said image file” is taught in '249 col. 7 lines 16-18 “The extracted stamping information 302 (202) can be

displayed to show ownership information on the computer display monitor in block 303."

13. **As to independent claims 11-13, 16-18, and 27-29** these claims hold the same limitations as cited in claims above are therefore rejected using the same rationale.
14. **As to dependent claims 14, 15, 19, 20, 30, and 31** these claims hold the same limitations as cited in claims above are therefore rejected using the same rationale.

Claim Rejections - 35 USC § 103

15 The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

16. **Claim 32** is rejected under 35 U.S.C. 103(a) as being unpatentable over '249, in view of Wong U.S. Patent No. 6,504,941 (hereinafter '941).

17. **As to dependent claim 32, "An image processing system as claimed in claim 1 or 2" has been rejected in reference to '249 as cited above in paragraph numbers 5 and 6, the following in italics is not taught in exact terminology in '249**

- "wherein: said image providing apparatus defines a location information for embedding said digital watermark in a part of a region in said image file and provides said image file in which said digital watermark is embedded based on said location

information" is taught in '941 col. 4, lines 51-54 "wherein the output of the means for combining is a combined image block; and a means for inserting 126 the combined image block (C.sub.r) into the modified image block X.sub.r, wherein the means for inserting 126 the combined image block (C.sub.r) into the modified image block X.sub.r is electrically coupled to the means for modifying 110 at least one predetermined bit of the image block";

- *"said image utilizing apparatus extracts said digital watermark from said image file provided by said image providing apparatus based on said location information"* is disclosed in '941 col. 8, lines 20-25 "Referring to FIG. 2A and the flowchart shown in 2B shows a method of extracting a watermark from a digital image Y.sub.r, including the steps of: for each I.times.J block, modifying at least a predetermined bit of the watermarked image Y.sub.r to a predetermined value (step 252), wherein the modified watermarked image Y.sub.r is Y.sub.r ; extracting at least a predetermined bit from the watermarked image (step 254)";

- *"verifies whether a data in said part of a region, in which said digital watermark is embedded, has been tampered"* is shown in '941 col. 8 lines 41-49 "After we have obtained the extracted watermark, the extracted watermark can be compared (visually, via a computer image comparison program, etc.) to an appropriate watermark. For example, the appropriate watermark may be an image transmitted to the receiver at an earlier time for watermark comparison purposes. If there is deviation between the two watermarks, then the locations of the deviations indicate the regions within the watermarked image that have been changed".

- It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '249 that explain how watermarks are inserted and extracted into an image to include authentication method. One of ordinary skill in the art would have been motivated to perform such a modification because a method is needed to determine if image has been modified. As indicated by '941 (see col. 2, lines 34 et seq.) "A method of invisible watermarking that can be used both for purposes of ownership verification and authentication, that can detect changes in pixel values as well as image size, and that may be used in public key or alternatively, secret key watermarking systems is needed".

18. **Claim 33-63** are rejected under 35 U.S.C. 103(a) as being unpatentable over '249, in view of '941, further in view of Stefik U.S. Patent No. 6,233,684 B1 (hereinafter '684).

19. **As to dependent claim 33**, "An image processing system as claimed in claim 1 or 2" has been rejected in reference to '249 as cited above in paragraph numbers 5 and 6,

- "and verifies whether a data in said part of a region, in which said digital watermark is embedded, has been tampered" *is taught in '941 col. lines 8 lines 41-49* "After we have obtained the extracted watermark, the extracted watermark can be compared (visually, via a computer image comparison program, etc.) to an appropriate watermark. For example, the appropriate watermark may be an image transmitted to the receiver at an earlier time for watermark comparison purposes. If there is deviation

between the two watermarks, then the locations of the deviations indicate the regions within the watermarked image that have been changed";

- the following in italics is not taught in exact terminology in the combination of teaching from '249 and '941:

- "wherein: said image providing apparatus recognizes a format of said image file, and provides said image file in which said digital watermark is embedded in a part of a region based on said format and said image utilizing apparatus recognizes said format of said image file provided by said image providing apparatus, extracts said digital watermark from said part of a region based on said format" is taught in '684 col. 1, lines 54-65 "The term fingerprint is sometimes used in contrast with watermarks to refer to marks that carry information about the end user or rendering event rather than the document or publisher. These marks are called "fingerprints" because they can be used to trace the source of a copy back to a person or computer that rendered the original. The same technologies and kinds of marks can be used to carry both watermark and fingerprint information. In practice, it is not only possible but often desirable and convenient to combine both kinds of information--for watermarks and fingerprints--in a single mark".

- It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '249 and '941 that explain how watermarks are inserted and extracted into an image in a specific location to include a method of determining the provider of the information. One of ordinary skill in the art would have been motivated to perform such a modification because this information helps protect

digital works from being copied or unauthorized alterations. As indicated by '684 (see col. 4, lines 52 et seq.) "A trusted rendering device for minimizing the risk of unauthorized copying of rendered digital works is described. The risk of unauthorized copying of digital documents comes from three main sources: interception of digital copies when they are transmitted (e.g., by wiretapping or packet snooping); unauthorized use and rendering of digital copies remotely stored, and unauthorized copying of a rendered digital work. The design of trusted rendering devices described herein addresses all three risks".

20. **As to independent claims 34 and 35** these claims hold the same limitations as cited in claims above are therefore rejected using the same rationale.

21. **As to dependent claim 36**, "wherein said image providing apparatus provides said image file in which a different kind of said digital watermark is embedded in a different region in said image file" is shown in '684 col. 8 lines 41-64 "A key concept in governing sale, distribution, and use of digital works is that publishers can assign "rights" to works that specify the terms and conditions of use. These rights are expressed in a rights language as described in the aforementioned U.S. Pat. No. 5,629,980. The currently preferred grammar is provided herein in Appendix A. It is advantageous to specify watermark information within a rendering or play right within the grammar for a number of reasons. First, specification in this manner is technology independent. So different watermarking technologies may be used or changed without

altering the digital document. Second, multiple watermarking technologies may be applied to the same digital work, e.g. a visible watermarking technology and an invisible watermarking technology. So if the visible watermark is removed, the invisible one may remain. Third, the watermark information to be placed on the digital work can be associated with the rendering event, rather than the distribution event. Fourth, the watermark information can be extended to include the entire distribution chain of the digital work. Fifth, security and watermarking capabilities of a rendering system may be specified as a condition of rendering. This will further insure the trusted rendering of the digital work".

22. **As to dependent claim 37**, "wherein said image providing apparatus provides said image file in which P a different kind of said digital watermark is embedded according to an image quality in each region where said digital watermark is embedded" is disclosed in '941 col. 2 lines 29-33 "The watermark insertion procedure computes a hash function of a modified image block, a key and various image parameters, and then combines the hashed output with a block of the watermark bitmap, resulting in a combined image block".

23. **As to dependent claim 38**, "wherein: said location information for embedding a digital watermark includes a location information of a region for displaying a specific information necessary for detecting a tamper" is taught in '941 col. 8 lines 41-49 "After we have obtained the extracted watermark, the extracted watermark can be compared

(visually, via a computer image comparison program, etc.) to an appropriate watermark. For example, the appropriate watermark may be an image transmitted to the receiver at an earlier time for watermark comparison purposes. If there is deviation between the two watermarks, then the locations of the deviations indicate the regions within the watermarked image that have been changed”;

“said image utilizing apparatus extracts said digital watermark with said message digest from said image file based on said location information” is shown in ‘941 col. 8, lines 25-29 “extracting at least a predetermined bit from the watermarked image (step 254); calculating a digest of the values using a cryptographic hash function (step 256); combining the hashed output with the image block E.sub.r”;

“generates a corresponding message digest using said specific information in said provided image file, and detects tampering with said image file by comparing said extracted message digest With said corresponding generated message digest” is disclosed in ‘941 col. 9, lines 39-40 “That is, the digest generated from both image blocks must be identical”.

24. **As to dependent claim 39**, this claim holds the same limitations as cited in claims above and is therefore rejected using the same rationale.

25. **As to dependent claim 40**, “wherein said region for embedding said message digest corresponding to said specific information is independent of said region for

displaying said specific information necessary for detecting said tamper" is disclosed in '941 col. 2 lines 21-29 "The present invention provides an invisible digital watermarking technique that can serve the two purposes of ownership verification and authentication, that can detect changes in pixel values as well as image size, and that may be used in public key or alternatively, secret key watermarking systems. The present invention includes a watermark insertion procedure used by the image owner and a corresponding extraction procedure used by the receiver of the image".

26. **As to dependent claim 41** "wherein: said location information is registered in both of said image providing apparatus and said image utilizing apparatus said image providing apparatus embeds said digital watermark in said image file based on said registered location information; and said image utilizing apparatus extracts said digital watermark from said image file based on said registered location information" is taught in '941 col. 8, lines 44-49 "For example, the appropriate watermark may be an image transmitted to the receiver at an earlier time for watermark comparison purposes. If there is deviation between the two watermarks, then the locations of the deviations indicate the regions within the watermarked image that have been changed".

28. **As to independent claims 43, 44, 49, 50, 58, 61, and 62**, these claims hold the same limitations as cited in claims above are therefore rejected using the same rationale.

29. **As to dependent claims 42, 45-48, 51, 54-57, 60 and 63** these claims hold the same limitations as cited in claims above are therefore rejected using the same rationale.

30. **As to independent claims 21-26, 52, 53, and 59,** "A recording medium storing a program to be executed by a computer, said program comprising" is taught in '941 col. 12, lines 29-33 "Alternatively, in another embodiment, the implementation of the block diagram shown in FIG. 1A could be implemented entirely in software, wherein the software is stored on a computer readable media and is adapted to running on a computer system" the remainder or the text in these claims hold the same limitations as cited above and is therefore rejected.

Conclusion

31. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (703) 305-8917. The examiner can normally be reached on 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 306-5484.


1/12/87
NORMAN M. WRIGHT
PRIMARY EXAMINER


12 JAN 2004